CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

ANPD: International Transfers of Personal Data

June 30, 2022

I. INTRODUCTION

In response to the Brazilian Data Protection Authority's (ANPD) request for feedback on its development of regulations regarding international transfers of personal data, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The ANPD has written a thoughtful set of questions regarding international data transfers. We understand that the ANPD is seeking answers to those questions, as well as other items the ANPD should take into consideration. In this regard, we do not have feedback on all of the ANPD's specific questions but, we do want to offer several points that may be of value in developing regulations on international data transfers. In particular, modern IT architecture and cybersecurity are dependent upon international data flows, and it is important to incentivize and empower organizations in Brazil to utilize state-of-the-art solutions.

A. International Data Transfers

i. Current Obstacles

We commend the ANPD for asking for feedback on any obstacles companies currently face when transferring data between Brazil and other countries. One of the lessons learned from the European Union is the difficulty of relying on a "white list approach," where a small number of countries are designated as providing parity in the data laws of another country. The difficulty with this approach is two-fold. First, instead of relying upon a single international standard, such approaches create competing standards for adequacy that may or may not take into account a holistic approach to data protection in another jurisdiction nor other risk-mitigation measures related to data flows. Second, current experience has demonstrated that approval processes can be burdensome for both the applicant country and the host data protection authority. Brazil's economy is dependent upon global data flows, and relying upon a white list approach can take years of administrative time, as it involves review and complex analysis of legal regimes that are often not static. The white list approach creates obstacles that can inhibit Brazilian companies, organizations and public sector bodies from engaging in cross border data flows and even accessing key technologies.

ii. Transfer Mechanisms

a. Contractual Agreements

CrowdStrike agrees that one way to adequately protect cross-border transfers of personal information is in the form of written agreements, specifically, contractual agreements. Each of these parties, controllers, processors, and subprocessors, are contractually bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability." Moreover, each party must abide by its own LGPD requirements in a "Chain of Independent Obligations." In other words, data subject rights remain protected by (i) enforceable contractual obligations between respective parties, and (ii) direct application of LGPD to any party processing personal data within the scope of LGPD.

Where both the Chain of Contractual Accountability and the Chain of Independent Obligations exist, the legal position of the data subject is adequately protected. For example, a controller that is party to a Data Processing Agreement with a processor will afford protections to its own data subjects because the processor is also obligated to obtain commitments from its own processors that process the

controllers' data. Acting in concert with these contractual protections, the parties' independent obligations under LGPD, including the requirements to establish a compliant LGPD program and deploy state-of-the-art and risk appropriate security safeguards in line with LGPD Art. 6 and Art. 46, act to further strengthen the protection of personal data and the legal rights of data subjects. Ultimately, existing, well-established concepts of privity of contract coupled with LGPD's direct application to global processing activities provide sufficient protections for data subjects.

b. Standard Contractual Clauses

Another transfer mechanism that the ANPD specifically asked for feedback on are Standard Contractual Clauses (SCC). Regarding SCCs, we have a few points. SCCs are reliable, easy to use and manageable. As the ANPD considers developing and implementing SCCs, we emphasize that SCCs should be written with flexibility in mind and should, as an international transfer mechanism, be multilingual. When parties have the flexibility to negotiate contractual terms, they may be customized to specific use cases and technological designs. Accordingly, SCCs written with narrow specifications and rigid obligations risk being impractical with the realities of the data flows they seek to protect.

B. Importance of cybersecurity

Supporting contractual agreements and SCCs can be done with a strong policy on cybersecurity. Cross-border data flows are necessary for cybersecurity. In fact, many of the most innovative technologies for protecting personal data against data breaches leverage endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general often invariably involves cross-border data transfers.

We recommend considering the importance of cybersecurity as a supplemental measure to the written agreements by looking at threats, predominantly in terms of threat actors. Malware, malicious infrastructure, and adversary tactics, techniques, and procedures (TTPs) change over time, but often the groups behind malicious activities are more durable. This means that considering threat actor motivations

helps defenders understand everything from their incentives to the risks posed by failing to prevent them from breaching your environment. Threat actors generally fall into the categories of: criminal groups, which largely seek profit; nation state entities, which pursue a variety of geopolitical ends; and 'hacktivists,' which have ideological motives. When crafting guidance, governments must be concerned with each, particularly during a time of unprecedented attacks from specific nation states along with the general trend of increased e-crime.

Specific threats vary across these different types of actors, but a few are especially notable. Criminal groups increasingly target public sector entities with ransomware, which disrupts victim IT environments in order to extort funds. Nation state groups have also used ransomware-like tools and TTPs to cause disruptions for other ends. Additionally, nation states have been observed to hack and leak sensitive communications for political ends, or steal intellectual property or sensitive business information to strengthen domestic commercial actors. Across all types of threat groups, adversaries are leveraging TTPs that enable them to avoid using malware, which complicates detection and prevention for entities using unsophisticated or legacy security solutions.

Further, we advocate for speed based cybersecurity metrics such as the "1-10-60 Rule."[1] This concept holds that security teams should endeavor to reliably detect malicious events within one minute; investigate them within ten minutes; and isolate or remediate affected hosts or resources within one hour. Further, organizational leaders should measure each of these performance indicators over time, and continuously improve them until the goals are met. Organizations that can defend themselves at this velocity will be well-equipped to outpace the vast majority of threat actors,[2] and prevent minor security events from becoming costly, complex, and sometimes devastating incidents.

That being said, we believe today's economy depends more than ever before on cross-border data flows and data portability. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from

[1] A more in-depth explanation of this concept is available here: https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/.
[2] *See* CrowdStrike's 2020 Global Threat Report: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.

anywhere" movement. The importance of cross-border data flows is far-reaching, and affects individuals, entities, and society more broadly. Any restriction on cross-border data flow or data portability requirements could have adverse implications for Brazil's innovation, jobs, access to services, and effective cybersecurity. This means that it is critical to provide organizations with deference to make their own context-informed–and critically, risk-informed–decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers.

Data protection is best achieved where intentional transfers of personal data are permitted with practical safeguards, while unintentional transfers of personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to personal data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules

III. CONCLUSION

Cyber attacks from advanced nation-state actors, criminal groups, and hacktivists pose a substantial threat to the safety of personal and other sensitive data. Therefore, cybersecurity should play a critical role in and is thus critical when developing regulations on international transfers of personal data. As the ANPD develops its regulations on international data transfers, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on

or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

IV. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Dr. Christoph Bausewein, CIPP/E
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

***